IS-IS 認証の設定

内容

概要

ルーティング テーブルに悪意のある情報が混入しないようにするために、ルーティング プロトコルの認証を設定することを推奨します。このドキュメントでは、IP 用の Intermediate System-to-Intermediate System（IS-IS）を実行しているルータ間のクリア テキスト認証について説明します。

このドキュメントでは、IS-ISクリアテキスト認証についてのみ説明します。他のタイプのIS-IS認証の詳細は、『IS-ISネットワークにおけるセキュリティの強化』を参照してください。

前提条件

要件

このドキュメントの読者は、IS-ISの動作と設定に精通している必要があります。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。このドキュメントの設定は、Cisco IOSバージョン12.2(24a)が稼働するCisco 2500シリーズルータでテストされています

背景説明

IS-ISでは、指定したリンク、エリア、またはドメインのパスワードを設定できます。ルータ同士が隣接関係を結びたい場合、それぞれのルータで設定されている認証のレベルに対して同じパスワードを交換する必要があります。適切なパスワードが設定されていないルータは、対応する機能（回線の初期化、エリアのメンバになること、レベル 2 のドメインのメンバになることなど）に関与することが禁止されます。

Cisco IOS® ソフトウェアでは、3種類のIS-IS認証を設定できます。

- **IS-IS認証**：これは長い間、IS-ISの認証を設定する唯一の方法でした。
- **IS-IS HMAC-MD5認証**：この機能は、各IS-ISプロトコルデータユニット(PDU)にHMAC-MD5ダイジェストを追加します。 これはCisco IOSソフトウェアバージョン12.2(13)Tで導入され、サポートされているプラットフォームの数は限られています。
- **拡張クリアテキスト認証**：この新機能を使用すると、ソフトウェア設定の表示時にパスワードを暗号化できる新しいコマンドを使用して、クリアテキスト認証を設定できます。また、パスワードの管理と変更が容易になります。

注：ISIS MD**-5およ**び拡張クリアテキスト認証に関する情報は、『IS-ISネットワークにおけるセキュリティ強化』を参照してください。

IS-ISプロトコルは、RFC 1142で規定されているように、LSPの一部として認証情報を含めることで、HelloおよびリンクステートパケットLSP)の認証を提供します。この認証情報は、Type Length Value（TLV）の 3 つの組み合わせとして符号化されています。認証TLVのタイプは10です。TLVの長さは可変です。TLVの値は、使用されている認証タイプによって異なります。デフォルトでは、認証は無効にされています。

設定

この項では、リンク、エリア、およびドメインに対してIS-ISクリアテキスト認証を設定する方法について説明します。

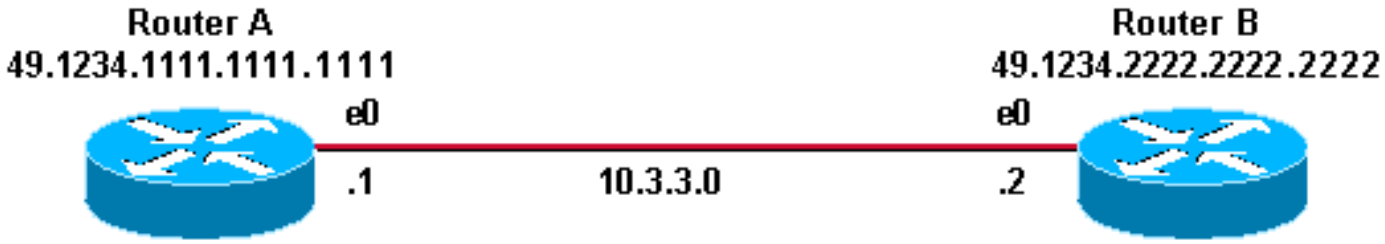
注：このドキュメントで使用されているコマンドの詳細を調べるには、コマンドの検索に関するベストプラクティス(登録ユーザーのみ)を使用してください。

インターフェイス認証

インターフェイスでIS-IS認証を設定すると、レベル1、レベル2、またはレベル1/レベル2の両方のルーティングに対してパスワードを有効にできます。レベルを指定しない場合、デフォルトはレベル1とレベル2です。認証が構成されているレベルに応じて、パスワードは対応するHelloメッセージで伝送されます。IS-IS インターフェイス認証のレベルは、そのインターフェイスでの隣接関係のタイプと一致している必要があります。**show clns neighborコマンド**を使用して、隣接関係のタイプを確認します。エリアやドメイン認証には、レベルを指定することはできません。

ネットワーク図、およびルータ A の Ethernet 0 とルータ B の Ethernet 0 でのインターフェイス認証の設定は次のとおりです。ルータAとルータBの両方で、レベル1とレベル2の両方にisisパスワードSECr3tが設定されています。これらのパスワードでは大文字と小文字が区別されます。

Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）の IS-IS を使用して設定されたシスコ ルータ間では、CLNS 隣接関係はデフォルトで レベル 1 またはレベル 2 となります。したがって、ルータ A およびルータ B では、レベル 1 またはレベル 2 のいずれか一方だけが特別に設定されない限り、両方のタイプの隣接関係を持つことになります。



ルータ A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
```

ルータ B

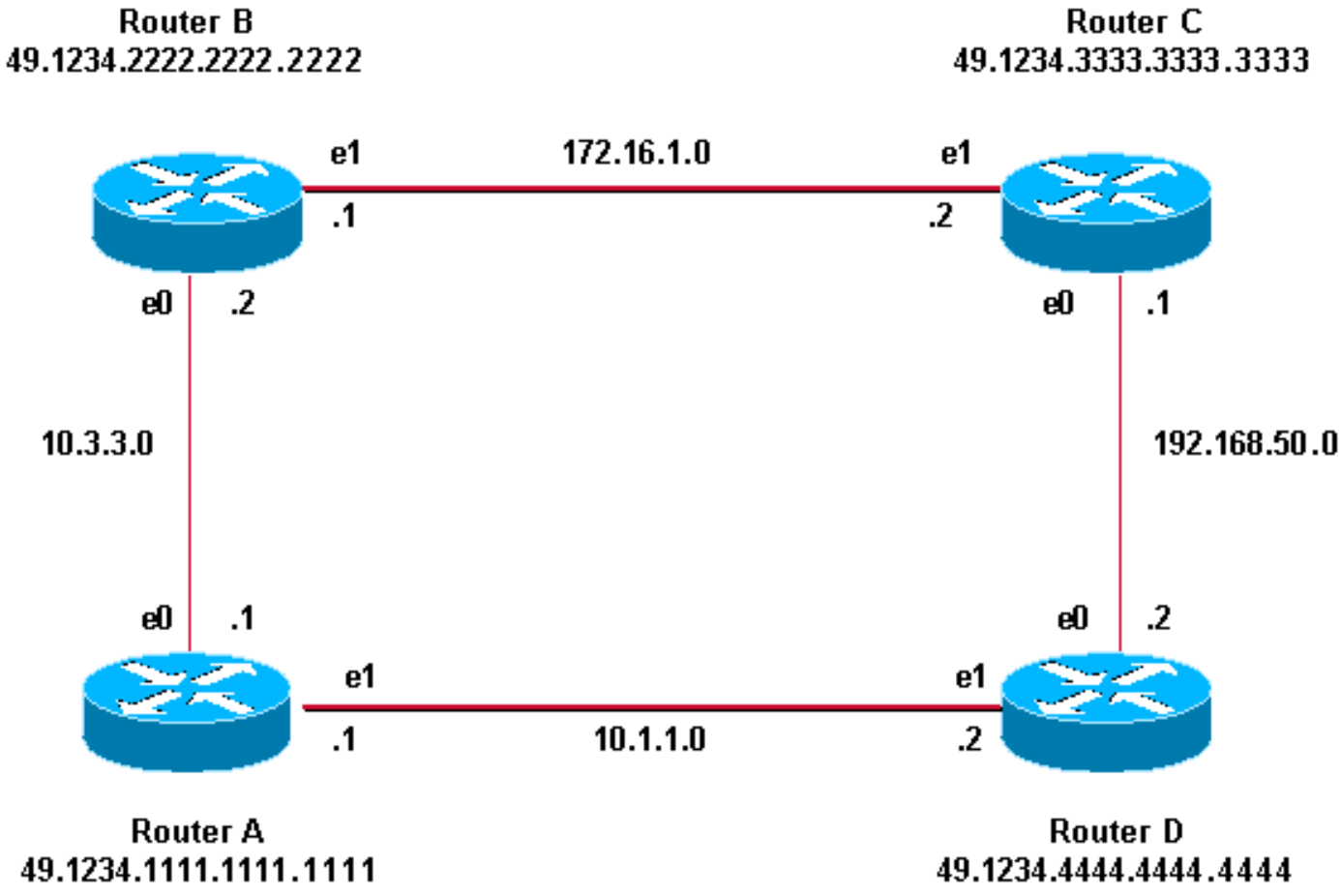
```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
isis password SECr3t

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

エリア認証

エリア認証に関するネットワーク図と設定を次に示します。エリア認証が設定されると、パスワードはL1 LSP、CSNP、およびPSNPSで伝送されます。すべてのルータが同一の IS-IS エリアである 49.1234 に属し、またすべてのルータに対してエリア パスワードとして「tiGHter」が設定されています。



ルータ A

ルータ B

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
area-password tiGHter
```

ルータ C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.1 255.255.255.0
ip router isis

router isis
net 49.1234.3333.3333.3333.00
area-password tiGHter
```

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
area-password tiGHter
```

ルータ D

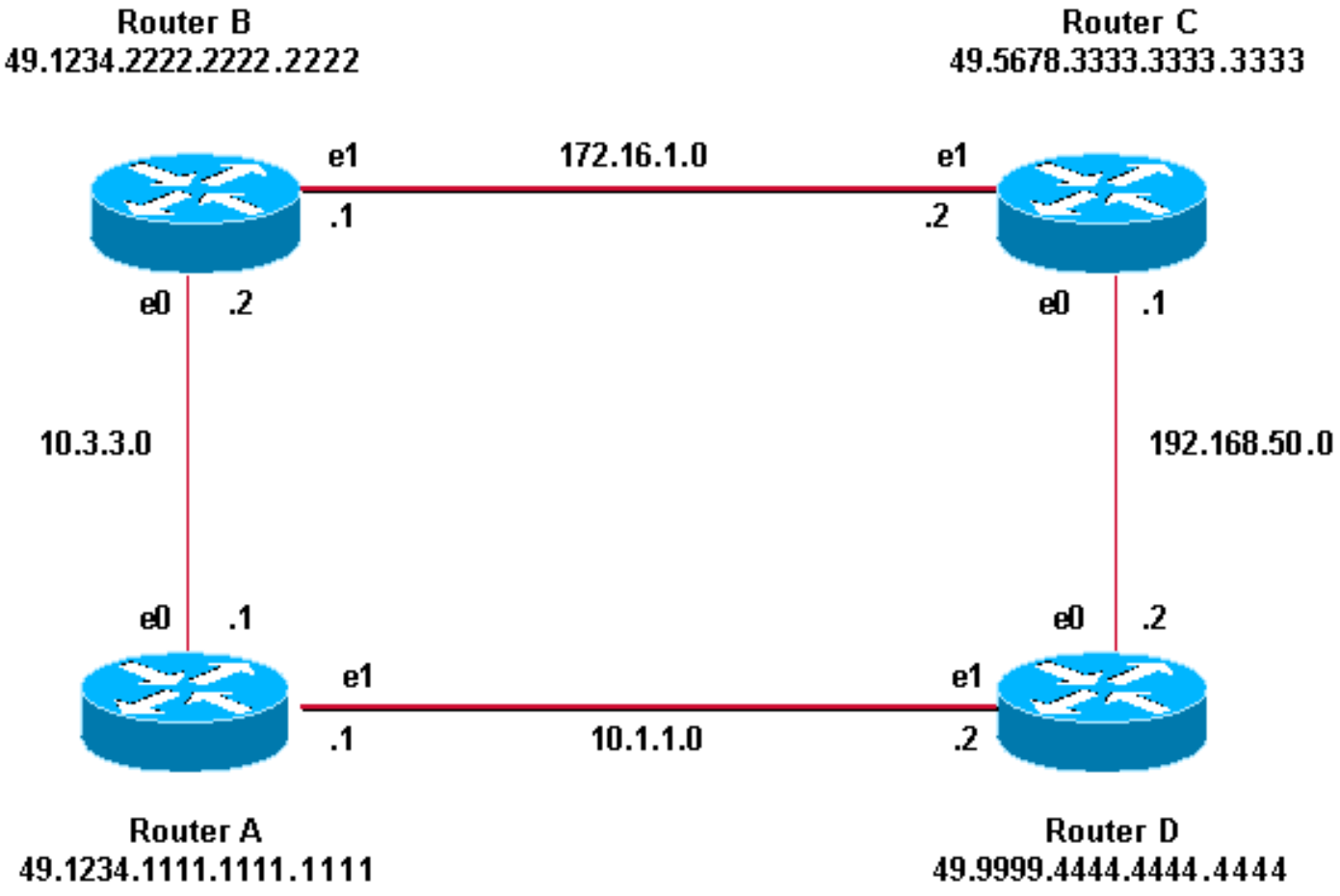
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis

router isis
net 49.1234.4444.4444.4444.00
area-password tiGHter
```

ドメイン認証

ドメイン認証に関するネットワーク図と設定を次に示します。ルータAとルータBはIS-ISエリア49.1234にあります。ルータCはIS-ISエリア49.5678にあります。ルータDはエリア49.9999にあります。すべてのルータは同じIS-ISドメイン(49)にあり、ドメインパスワード「seCurity」が設定されています。



ルータ A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
domain-password seCurity
```

ルータ B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis
interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
domain-password seCurity
```

ルータ C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.1 255.255.255.0
ip router isis

router isis
net 49.5678.3333.3333.3333.00
domain-password seCurity
```

ルータ D

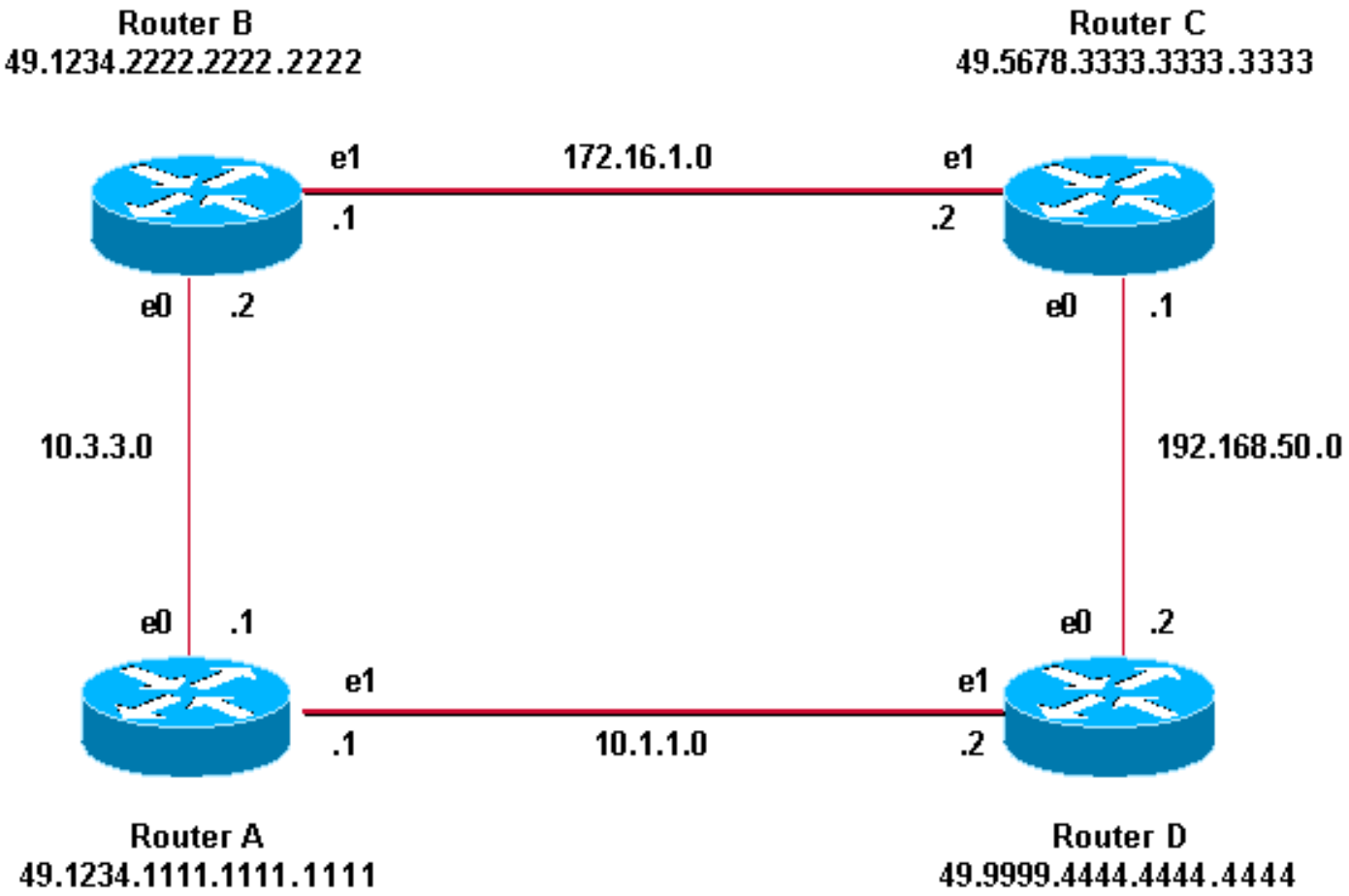
```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis

router isis
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

ドメイン、エリア、インターフェイス認証の組み合わせ

このセクションのトポロジと部分的な設定は、ドメイン、エリア、およびインターフェイス認証の組み合わせを示しています。ルータ A とルータ B は同じエリアにあり、エリア パスワード「tiGHter」が設定されています。 ルータCとルータDは、ルータAとルータBとは2つの異なるエリアに属しています。すべてのルータが同じドメインにあり、ドメインレベルのパスワードとして「seCurity」を共有しています。 ルータ B とルータ C には、これらの間でイーサネット回線が設定が行されています。ルータCとルータDは、ネイバーとL2隣接関係のみを形成し、エリアパスワードの設定は不要です。



ルータ A

```
interface ethernet 0
ip address 10.3.3.1 255.255.255.0
ip router isis
interface ethernet1
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
domain-password seCurity
area-password tiGHter
```

ルータ B

```
interface ethernet 0
ip address 10.3.3.2 255.255.255.0
ip router isis

interface ethernet1
ip address 172.16.1.1 255.255.255.0
ip router isis
clns router isis
isis password Fri3nd level-2

router isis
net 49.1234.2222.2222.2222.00
domain-passwordseCurity
area-password tiGHter
```

ルータ C

```
interface ethernet1
ip address 172.16.1.2 255.255.255.0
ip router isis
isis password Fri3nd level-2

interfaceethernet0
ip address 192.168.50.1 255.255.255.0
ip router isis

router isis
net 49.5678.3333.3333.3333.00
domain-password seCurity
```

ルータ D

```
interface ethernet1
ip address 10.1.1.2 255.255.255.0
ip router isis

interface ethernet0
ip address 192.168.50.2 255.255.255.0
ip router isis

router isis
net 49.9999.4444.4444.4444.00
domain-password seCurity
```

確認

特定のshowコマンドは、Cisco CLI Analyzer(登録ユーザ専用)でサポートされています。このコマンドを使用すると、showコマンドの出力を分析できます。

インターフェイス認証が正常に動作しているかどうかを確認するには、ユーザEXECモードまたは特権EXECモードでshow clns neighborsコマンドを使用します。コマンドの出力には、接続の隣接関係のタイプと状態が表示されます。show clns neighborsコマンドの次の出力例は、ルータがインターフェイス認証用に正しく設定され、状態がUPであることを示しています。

```
RouterA# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
RouterB        Et0         0000.0c76.2882  Up     27        L1L2 IS-IS
```

エリアおよびドメイン認証では、次のセクションで説明するように、debugコマンドを使用して認証の検証を行うことができます。

トラブルシュート

直接接続されたルータがリンクの一方の側で認証が設定されていて、もう一方の側では認証が設定されていない場合、ルータはCLNS IS-IS隣接関係を形成しません。次の図では、ルータ B では Ethernet 0 インターフェイスに対するインターフェイス認証が設定され、ルータ A では隣接するインターフェイスに認証が設定されていません。

```
Router_A# show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Router_B       Et0         00e0.b064.46ec  Init   265       IS   ES-IS

Router_B# show clns neighbors
```

直接接続されたルータのリンクの一方の側にエリア認証が設定されている場合、2つのルート間にCLNS IS-IS隣接関係が形成されます。ただし、エリア認証が設定されているルータは、エリア認証が設定されていないCLNSネイバーからのL1 LSPを受け入れません。ただし、エリア認証のないネイバーは、L1とL2 LSPの両方を引き続き受け入れます。

これは、エリア認証が設定され、エリア認証なしでネイバー（ルータB）からL1 LSPを受信するルータAのデバッグメッセージです。

```
Router_A# deb isis update-packets
 IS-IS Update related packet debugging is on
 Router_A#
 *Mar 1 00:47:14.755: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1128,
 *Mar 1 00:47:14.759: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
 *Mar 1 00:47:14.763: ISIS-Upd: LSP authentication failed
 Router_A#
 *Mar 1 00:47:24.455: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1118,
 *Mar 1 00:47:24.459: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
 *Mar 1 00:47:24.463: ISIS-Upd: LSP authentication failed
 RouterA#
```

あるルータでドメイン認証を設定すると、ドメイン認証が設定されていないルータからのL2 LSPが拒否されます。認証が設定されていないルータは、認証が設定されているルータからのLSPを受け入れます。

次のデバッグ出力では、LSP 認証の失敗を示しています。ルータCAはエリアまたはドメイン認証

用に設定されており、ドメインまたはパスワード認証用に設定されていないルータ（ルータDB）からレベル2 LSPを受信しています。

```
Router_A# debug isis update-packets
IS-IS Update related packet debugging is on
Router_A#
*Mar  1 02:32:48.315: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 374,
*Mar  1 02:32:48.319: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
*Mar  1 02:32:48.319: ISIS-Upd: LSP authentication failed
Router_A#
*Mar  1 02:32:57.723: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 365,
*Mar  1 02:32:57.727: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
*Mar  1 02:32:57.727: ISIS-Upd: LSP authentication failed
```

関連情報

- IP ルーティングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems